The Securities and Exchange Commission (SEC) Guidelines on Cybersecurity Framework for the Insurance Sector, 2020

1. Introduction

The increasing reliance of the insurance sector of Pakistan on the technology, in distribution and in offering other innovative products through usage of technology, makes it imperative that adequate measures must be taken to make its information technology systems, and of its partners and intermediaries, secure and resilient. This also makes it imperative to put regulatory measures in place for threat reduction, vulnerability reduction, deterrence and other cyber security measures. Accordingly, the Securities and Exchange Commission of Pakistan (SECP) is pleased to issue the SEC Guidelines on Cybersecurity Framework for the Insurance Sector, 2020 (the "Guidelines") specifying guiding principles for adoption of suitable cybersecurity measures. The SECP recognizes that while cybersecurity is necessary for all insurers, there is no one-size-fits-all prescription for insurers, rather it is dependent on the nature, size and complexity of the insurers business.

2. Applicability

These Guidelines will apply to all insurers, including takaful operators registered under the Insurance Ordinance 2000. These Guidelines will become effective from July 1, 2020; However, earlier adaption is encouraged.

3. Alignment of Cybersecurity Framework with overall Risk Management Framework

The insurers need to take into account the underlying cyber risk at the time of formulation of risk management policy by the Board of Directors (the "Board") of the insurer, as part of significant policy as required under the clause (xi) of the Code of Corporate Governance for Insurers, 2016. The Chief Information Security Officer (CISO) and the Risk Management Department (or function) will jointly identify, assess, quantify, monitor, and control the nature, significance and interdependencies of the cyber risks and will be required to develop a cybersecurity strategy and framework to be put in place for mitigation of inherent cyber risk.

4. Developing cybersecurity framework and mechanisms

Insurers, as a starting point, shall consider existing core technical standards on cybersecurity such as the National Institute of Standards and Technology (**NIST**) **Cybersecurity Framework**, and Information Systems Audit and Control Association (**ISACA**)'s COBIT ("Control Objectives for Information and Related Technologies"), and the International Organisation for Standardisation (**ISO**) **27000 series**, which consist of a set of standards and best practices to manage cyber risks. In 2017, the Financial Stability Board (FSB) had also published a **Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices** to discuss cybersecurity in the financial sector. Further, International Association of Insurance Supervisors (IAIS) has published **Application Paper on Supervision of Insurer Cybersecurity, November 2018** which focuses on supervision (i.e. from regulatory perspective) of insurers' cybersecurity.

5. Appointment of Chief Information Security Officer (CISO)

(i) The insurers are encouraged to appoint or designate a senior officer as Chief Information Security Officer (CISO) having adequate qualification and experience, who will be responsible for implementation of overall cybersecurity framework within the organization. The insurer shall carryout, a well-documented and signed assessment of whether a separate CISO is required or not, taking into consideration the risks inherent in the organization with regards to the cybersecurity, and then based on the assessment may appoint/ designate a CISO, within three months of coming into effect of these Guidelines.

(ii) The Head of Information Technology Department (HoIT) of Insurer shall preferably not be appointed as CISO. Where the same person is appointed as both HoIT and CISO or a senior person of the Information Technology department is appointed as CISO, it should be ensured that direct reporting lines of that person for both the roles are separate. Further, the CISO should report to the Board at least once a year.

6. Insurers to conduct cyber risk assessment

(i) Insurers should implement annual assessment programs to help the Board and senior management evaluate and measure the adequacy and effectiveness of the insurer's cybersecurity framework .

(ii) The insurers shall submit to the Commission the cybersecurity framework assessment reports, formulated in compliance of the above clause, by April 30 of every year. The cybersecurity framework assessment report is required to be signed by the Chief Information Security Officer (CISO) and the Chief Operations Officer (COO)/ Chief Executive Officer (CEO) of the Company.

7. Data Security and Confidentiality

The insurer's cybersecurity framework should be able to protect the policyholder data in the wake of enhanced reliance on business process outsourcing (BPO), technology based agency arrangements and other strategic partnerships for offering technology based innovative insurance products and services.

8. Cyber risk insurance coverage

(i) All insurers should consider obtaining the cyber risk insurance to cover their own cyber risks, to which they are exposed. The purpose of cyber risk insurance is to mitigate losses from a variety of cyber incidents, including data breaches, business interruption, and network damage.

(ii) Purchasing cyber insurance does not remove the need for a sound control environment. Rather, cyber insurance may be a component of a broader risk management strategy and framework that includes identifying, measuring, mitigating, and monitoring cyber risk exposure. The insurer while weighing benefits and costs of purchasing cyber insurance should consider involving appropriate department across the organization, in the cyber insurance decision.

9. Insurers to have adequate cybersecurity systems in place

The insurers are required to have adequate network security and system security in place to safeguard their operating systems, software and databases against the cyber risks. The insurers will put in place secure configuration of hardware, operating systems, software, applications, databases and servers with all unnecessary services and programs disabled or removed. The insurers will ensure encryption at database level, storage level and during network transmission as per the classification and sensitivity of the data.

10. The Guiding Cybersecurity Framework for Insurance Sector

The insurers will formulate a sound cybersecurity framework in order to anticipate, withstand, detect, prevent and respond to cyber attacks in line with international standards and best practices. Few guiding principles in respect of formulation of cybersecurity framework are given in this section.

(A) Cybersecurity Strategy and Framework

(i) Cybersecurity strategies should clearly articulate principles regarding how the insurer intends to address cyber risks. The insurer's cybersecurity strategy should be closely aligned with, and complementary to, its cybersecurity framework, to ensure that the framework is capable of achieving its objectives.

(ii) The framework should support and promote both its operational security and the protection of policyholder data. Therefore, framework objectives should aim to maintain and promote the insurer's ability to anticipate, detect, withstand, contain and recover from cybersecurity incidents, so as to limit the likelihood or impact of a cybersecurity incident, which could damage the insurer's operations, its reputation, and the data privacy of its policyholders and third parties.

(iii) The framework should clearly define its objectives and horizon as well as the requirements for people, processes, and technology necessary for managing cyber risks and timely communication.

(iv) The framework must be supported by clearly defined roles and responsibilities of the insurer's Board and its management, and it is incumbent upon the Board and management to create a culture which recognizes that staff at all levels have important responsibilities in ensuring the insurer's cybersecurity.

(v) The framework should clearly articulate a plan for identification, assessment, measurement, monitoring, mitigation and management of cyber risks. The insurers should consider how the insurer would regularly review and actively mitigate the cyber risks that it bears from and poses to its stakeholders. The framework should be reviewed and updated with sufficient frequency to ensure that they remain effective.

(B) Governance

(i) The Board is ultimately responsible for setting strategy and ensuring that cyber risk is effectively managed. The Board should be regularly apprised of the insurer's cyber risk profile to ensure that it remains consistent with the insurer's risk tolerance as well as the insurer's overall business objectives.

(ii) The insurers need to define and facilitate performance of roles and responsibilities for officers implementing, managing, and overseeing effectiveness of cybersecurity strategy and framework to ensure accountability and to provide adequate resources, appropriate authority, and access to the governing authority e.g. board of directors.

(iii) An Board and senior management should cultivate awareness of and commitment to cybersecurity and should promote a culture that recognizes that staff at all levels have important responsibilities in ensuring the insurer's cybersecurity and lead by example.

(iv) Insurers should have in place information security policies, procedures and processes including definitions of roles and responsibilities across the organization. These policies, procedures and processes should include oversight of third party service providers, as well as cyber risk management processes and determination of priorities, constraints, assumptions, and risk tolerance level.

(C) Risk and Control Assessment

(i) Insurers should identify and classify functions including information assets and data sensitivity, as well as their interconnectedness; proactive technology and processes; external dependency management; and situational awareness.

(ii) The insurer should adequately account for cyber risks in its overall risk management system, identifying its business functions and supporting processes and conducting a risk assessment to understand the importance of each function and supporting processes. Identified business functions and processes should then be classified by insurers in terms of criticality, which in turn should guide the insurer's prioritization of its protection, detection, response, and recovery efforts.

(iii) To the extent practicable, the insurer should identify and maintain a current inventory or mapping of its information assets and system configurations, including interconnections with other internal and external systems including third party's systems. The inventory should encompass hardware, software platforms and applications, devices, systems, data, personnel, external information systems, critical processes, and documentation on expected data flows.

(iv) Insurers should identify and maintain a current record of both individual and system access rights. Insurers should integrate identification efforts with other relevant processes, such as acquisition and change management. Similarly, insurers should conduct business impact analysis for cyber risks.

(v) Insurers' risk profiles should identify key operational areas exposed to cyber risk, arising from both internal and external sources. Insurers should consider identification of cyber risks in its technologies and connection types; delivery channels for products and services; organizational characteristics (such as current or planned mergers, acquisitions, changes in IT environment, number of persons with privileged access, locations of operations and data centres, reliance on third party service providers etc.); and external threats.

(vi) Insurers should protect data both when at-rest, in-transit and in-storage commensurate with the criticality of the information held and associated classification, extending to backup systems and offline data stores as well.

(vii) Insurers should actively manage cyber risks presented by third parties and should verify that third-party service providers have implemented appropriate administrative, technical, and physical measures to protect and secure the data of an insurer and its customers to the same degree expected of the insurer.

(viii) An insurer should have appropriate situational awareness of the cyber risks that it faces. An insurer should seek to proactively identify cyber threats that could materially affect its ability to perform or to provide services as

expected, or that could have a significant impact on its ability to meet its obligations, including protection of confidential data. The insurer should regularly review and update this analysis.

(ix) Cyber threats to be considered should include those which could trigger extreme but plausible cyber events, even if they are considered unlikely to occur or have never occurred in the past.

(D) Monitoring and Testing

The insurers should establish systematic monitoring processes to rapidly detect cyber incidents and periodically evaluate the effectiveness of identified controls, including through network monitoring, testing, audits, and exercises.

(i) Insurers should protect network (hardware, firmware and software components) integrity including control of information flow, boundary protection, and network segregation if needed. Insurers should consider establishing a Security Operations Centre or developing similar capability to provide round the clock monitoring and such capabilities should be adaptively maintained and tested.

(ii) The insurers should be able to recognize signs of a potential cyber incident, or detect that an actual breach has taken place. An insurer should maintain effective capabilities to extensively monitor for anomalous activities.

(iii) The insurers should monitor relevant internal and external activities and events, seeking to detect vulnerabilities through a combination of signature monitoring for known vulnerabilities and behaviorally-based detection mechanisms. Insurers' detection capabilities should also address misuse of access by third party service providers, policyholders, potential insider threats, and other advanced threat activity through a strong cyber threat intelligence programme.

(iv) Insurers should manage the identities and credentials for physical, logical, and remote access to information assets, based on principles of least privilege and separation of duties. Insurers should take a defence-in-depth approach by instituting multi-layered detection controls covering people, processes, and technology, with each layer serving as a safety net for preceding layers.

(v) Insurer should consider placing an effective intrusion detection capability which may include data loss/leaks prevention and detection, the recording and documentation of audit logs, event data aggregation, correlation, analysis and communication, as well as network, personnel and external dependency activity monitoring.

(vi) The insurer should employ monitoring and detection capabilities to facilitate its incident response process and support information collection for the forensic investigation process.

(vii) Insurers should rigorously tests all elements of their cybersecurity framework to determine their overall effectiveness before being employed within an insurer, and regularly thereafter. The results should be communicated within the organization and should be used by the insurer to support the ongoing improvement of its cybersecurity. Proper procedures should be put in place to ensure that its Board and Senior Management are appropriately involved (e.g., as part of crisis management teams) and informed of test results.

(viii) The insurers should consider using a combination of the available state-of-the-art testing methodologies and practices which may include the following elements (which partly overlap and can be combined):

- Vulnerability assessments to identify and assess security vulnerabilities in the systems and processes.
- Scenario-based testing to address an appropriately broad scope of scenarios, including simulation of extreme but plausible cybersecurity incidents, and should be designed to challenge the assumptions of response, resumption, and recovery practices, including governance arrangements and communication plans.
- Penetration testing to identify vulnerabilities that may affect insurer's systems, networks, people or processes and to provide an in-depth evaluation of the security of insurers' systems.
- Red Team testing to challenge insurer's own organizations and external dependencies and to test for possible vulnerabilities and the effectiveness of an insurer's mitigating controls.
- Response testing to ensure effectiveness of insurer's response, resumption, and recovery plans and processes.
- Integrated or Dynamic testing to identify plausible complexities, dependencies and weaknesses that may have been overlooked in its recovery plans. Testing should include scenarios that cover breaches affecting external dependencies.

(E) Response

(i) The insurers should be able to implement incident response policies and other controls to facilitate effective incident response," and among other things, these controls should clearly address decision-making responsibilities, define escalation procedures, and establish processes for communicating with internal and external stakeholders."

(ii) Insurers should raise awareness among all its stakeholders by providing training for employees and others with access to its systems. Insurers should also develop response plans (Incident Response and Business Continuity) and communication plans which should be subject to review and improvement as appropriate.

(iii) Upon detection of a cybersecurity incident (or an attempt), an insurer should perform a thorough investigation to determine its nature and extent as well as the damage inflicted. The investigation should be followed by immediate actions to prevent further damage, and commence recovery efforts to restore operations based on its response planning.

(iv) Insurers should also be cognizant not to bring systems back up too quickly and risk another attack or expansion of the cybersecurity incident. Insurer should plan to resume critical operations as soon as is safely possible after a cybersecurity incident, it should analyse critical functions, transactions, and interdependencies to prioritize resumption and recovery actions while remediation efforts continue.

(v) Insurers should plan to have access to external experts, recognizing that a large-scale or industry wide event may reduce the availability of such key resources on short notice.

(vi) Insurers should develop and test response, resumption, and recovery plans. These plans should support objectives to protect the confidentiality, integrity, and availability of its assets, including policyholder data.

(vii) Insurers should consider implementing system and process design and controls for critical functions and operations to support incident response activities to the extent possible. An insurer's incident response, resumption, and recovery processes should be closely integrated with crisis management, business continuity, and disaster recovery planning and recovery operations, and coordinated with relevant internal and external stakeholders.

(viii) Insurers should have the capability to assist in or conduct forensic investigations of cyber incidents and engineer protective and detective controls to facilitate the investigative process.

(F) Recovery

(i) Insurers should have in place validated plans and procedures to recover from a cybersecurity incident. Cyber incident recovery arrangements should be designed to enable insurers to resume operations safely with a minimum of disruptions to policyholders and business operations. The recovery plans (Incident Recovery and Disaster Recovery) should be subject to review and improvement as appropriate

(ii) Insurers should design and test their systems and processes to enable timely recovery of accurate data following a breach. In addition, the insurer's cybersecurity framework should include data recovery measures, such as keeping a backup copy of all policyholder data in the event such data is corrupted.

(iii) In the event of a cyber incident where insurer's system and process are interconnected with third party service providers, an insurer should work with these third parties to resume operations in a safe manner.

(iv) Insurers should have formal plans for communicating with policyholders, internal and external stakeholders likely to sustain harm due to a major cybersecurity incident. Communication plans in accordance with governing law should be developed through an adaptive process informed by scenario-based planning and analysis as well as prior experience. Insurers should determine decision-making responsibilities for incident response and recovery in advance, and implement clearly defined escalation and decision-making procedures.

(G) Information Sharing

(i) Insurers should engage in the timely sharing of reliable, actionable cybersecurity information with internal and external stakeholders (including entities and public authorities within and outside the financial sector) on threats, vulnerabilities, incidents, and responses to enhance defenses, limit damage, increase situational awareness, and broaden learning.

(ii) Insurers should establish a process to gather and analyse relevant cyber threat information and should consider participating actively in information-sharing groups and collectives, within the country to gather, distribute and assess information about cyber practices, cyber threats, and early warning indicators relating to cyber threats. Insurers may participate in system-wide initiatives such as Incident Response Teams (IRT), if established through the joint efforts of insurers, or other financial institutions.

(iii) An insurer's analysis of cyber threat information should be in conjunction with other sources of internal and external business and system information.

(iv) An insurer's cyber threat intelligence operations should include the capability to gather and interpret information about relevant cyber threats posed by the insurer's third-party service providers, as well as utility providers and other critical infrastructure resources.

(v) An insurer should make cyber threat intelligence available to appropriate staff within the insurer with the responsibility for the mitigation of cyber risks at the strategic, tactical, and operational levels.

(vi) Insurers should plan for information-sharing through trusted channels, collecting and exchanging timely information that could facilitate the detection, response, resumption, and recovery of its own systems and those of other sector participants during and following a cybersecurity incident.

(vii) An insurer should consider exchanging information on its cybersecurity framework bilaterally with its third-party service providers to promote mutual understanding of each other's approach to securing systems that are linked or interfaced

(H) Continuous Learning

(i) Insurers should adopt a cybersecurity framework premised on ensuring continuous cybersecurity amid a changing threat environment. An insurer should implement an adaptive cybersecurity framework that evolves with the dynamic nature of cyber risks and allows the insurer to identify, assess, and manage security threats and vulnerabilities for the purpose of implementing appropriate safeguards into its systems.

(ii) Insurers should implement cyber risk management practices that go beyond reactive controls and include proactive protection against future cyber events.

(iii) Insurers should work towards achieving or acquiring predictive capabilities, capturing data from multiple internal and external sources, and defining a baseline for behavioural and system activity, including through outsourcing such expertise.

(iv) An insurer should systematically identify and distil key lessons from cyber events that have occurred within and outside the organization in order to advance its resilience capabilities.

(v) An insurer should actively monitor technological developments and keep abreast of new cyber risk management processes that can more effectively counter existing and newly developed forms of cyber attack. An insurer should consider acquiring such technology and know-how to maintain its cybersecurity, including through outsourcing such expertise.

(vi) Insurers may consider using metrics to assess cybersecurity maturity against a set of predefined criteria, such as operational reliability objectives.

****This paper ends here****